UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN RE THE ESTÉE LAUDER CO., INC. SECURITIES LITIGATION	No. 1:23-cv-10669-AS Hon. Arun Subramanian

ELECTRONIC DISCOVERY AGREEMENT AND [~~PROPOSED~~] ORDER

This Agreement and [Proposed] Order will govern how the parties manage electronic discovery in the above-captioned case.

I. IDENTIFICATION OF RESPONSIVE DOCUMENTS

The parties shall meet and confer in an effort to conduct discovery in the most efficient and effective manner. Specifically, the parties will attempt in good faith to come to an agreement on search and culling methods used to identify responsive information. The parties will meet and confer regarding any proposed limitations on the scope of discovery, including custodians, custodial and non-custodial sources, date ranges, file types, or any additional proposed method to cull documents for review (*e.g.*, search terms, technology-assisted review, predictive coding). The parties will not seek Court intervention regarding the methodology to be used to identify responsive information without first attempting to resolve any disagreements in good faith, based upon all reasonably available information.

The parties will meet and confer regarding the scope of preservation as required by Rule 26(f)(3)(C) of the Federal Rules of Civil Procedure.

A. Search Terms

Where the parties agree that potentially responsive ESI shall be searched through the use of search terms, the parties shall use the process identified below and shall meet and confer regarding any proposed deviation.

1. The producing party shall provide a list of proposed search terms, which shall contain all search terms that it believes would lead to the identification of relevant documents.

2. Upon receipt of the proposed search terms, the receiving party shall provide any additional search terms to identify responsive documents.

3. Upon receipt of the additional search terms, the producing party will provide a search term hit list or hit report after global de-duplication, including the number of documents that hit on each term, the number of unique documents that hit on each term (documents that hit on a particular term and no other term on the list), and the total number of documents that would be returned by using the proposed search term list, with and without families. In addition to global de-duplication, if the producing party intends to apply email thread suppression to its review population, the producing party may implement email thread suppression in connection with generating its search term hit list or hit report. When providing a hit list or hit report as described in this paragraph, each party must indicate whether its hit report accounts for email thread suppression or not.

4. The parties shall then meet and confer regarding the proposed search terms.

B. Technology-Assisted Review

A producing party may use predictive coding/technology-assisted-review or artificial intelligence for the purpose of culling the documents to be reviewed or produced, subject to (i) notifying the receiving party that it intends to use such technology and disclosing the name of the review tool, and (ii) the parties agreeing on a protocol for the use of such technologies. If the Parties cannot agree on a mutually agreeable protocol, the objecting party may initiate the Court's process for resolving any disputes regarding the use of such technology.

II. PRODUCTION OF HARD-COPY DOCUMENTS – FORMAT

Hard-copy documents should be scanned as single-page, Group IV, 300 DPI TIFF images with an .opt image cross-reference file and a delimited database load file (*i.e.*, .dat). The database load file should contain the following fields: "BEGNO," "ENDNO," "PAGES," "VOLUME," and "CUSTODIAN." The documents should be logically unitized (*i.e.*, distinct documents shall not be merged into a single record, and single documents shall not be split into multiple records) and be produced in the order in which they are kept in the usual course of business. If an original document contains color, and the color is necessary to understand the meaning or content of the document, the parties reserve the right to request that the affected documents be re-produced. Multi-page OCR text for each document should also be provided. Settings such as "auto-skewing" and "auto-rotation" should be turned on during the OCR process. If the settings on productions of hard-copy documents under this Section render the meaning or content of certain documents difficult or impossible to understand, the parties reserve the right to request that the affected documents be re-produced; to the extent there is a dispute about the necessity of reproduction of any hard-copy documents for quality issues, the parties agree to meet and confer in good faith.

III. PRODUCTION OF ESI

A. Format

Except where otherwise noted in this section, the parties will produce ESI in single-page, black and white, TIFF Group IV, 300 DPI TIFF images. Spreadsheet and presentation-type files, audio and video files, photo or graphic images, and documents with tracked changes in the metadata shall be produced in native format. Text messages, WhatsApp, Slack, iMessage, Teams, G-Chat, and Instant Bloomberg ("Short Message Communications"), where applicable, will be produced in as TIFF images of the RSMF with all available metadata and attachments. Except for messages that contain privileged content, Short Message Communications will be produced as complete communications, separated into 12-hour increments. To the extent Short Message Communications cannot be provided in TIFFs of RSMF, the parties shall meet and confer on the appropriate metadata fields and format of production. The parties are under no obligation to enhance an image beyond how it was kept in the usual course of business. TIFFs/JPGs will show any and all text, hidden content, and images that would be visible to the reader using the native software that created the document. For example, TIFFs/JPGs of email messages will include the BCC line, and documents will display comments and hidden content. If the image does not accurately reflect the document as it was kept in the usual course of business, including all comments, edits, tracking, etc., the parties agree to meet and confer in good faith on production format options. If the settings on productions of ESI under this Section render the meaning or content of certain documents difficult or impossible to understand, the parties reserve the right to request that the affected documents be re-produced; to the extent there is a dispute about the necessity of reproduction of any hard-copy documents for quality issues, the parties agree to meet and confer in good faith.

If a document is produced in native format, a single-page Bates stamped image slip sheet should be provided stating the document has been produced in native format, as applicable, with the exception of PowerPoint presentations. PowerPoint documents should be produced in native format along with single-page, 300 DPI TIFF/JPG images which display both the slide and speaker's notes. Each native file should be named according to the Bates number it has been assigned and should be linked directly to its corresponding record in the load file using the NATIVELINK field. The parties retain the right to request that additional documents or classes of documents, not already identified within this protocol, should be produced in native format; to the extent a party believes that a document or class of documents not already identified in this paragraph should be produced in native format, the parties agree to meet and confer in good faith.

B. De-Duplication and De-NISTing

Each party shall remove exact duplicate documents based on MD5 or SHA-1 hash values, at the family level. Attachments should not be eliminated as duplicates for purposes of production, unless the parent email and all attachments are also duplicates. The parties agree that an email that includes content in the BCC or other blind copy field shall not be treated as a duplicate of an email that does not include content in those fields, even if all remaining content in the email is identical.

The parties may use email thread suppression to avoid review and production of information contained within an existing email thread in another document being reviewed and produced, but shall not use email thread suppression to eliminate (a) the ability of a requesting party to identify every custodian who had a copy of a produced document or email, or (b) remove from a production any unique branches and/or attachments contained within an email thread.

De-duplication will be done across the entire collection (global de-duplication) and the CUSTODIAN-ALL field will list each custodian, separated by a semicolon, who was a source of that document and the FILEPATH-DUP field will list each file path, separated by a semicolon, that was a source of that document. Should the CUSTODIAN-ALL or FILEPATH-DUP metadata fields produced become outdated due to rolling productions, an overlay file providing all the custodians and file paths for the affected documents will be produced prior to substantial completion of the document production.

ESI may be de-NISTed using the industry standard list of such files maintained in the National Software Reference Library by the National Institute of Standards & Technology as it exists at the time of de-NISTing. Other file types may be added to the list of excluded files by agreement of the parties.

C. Metadata

All ESI will be produced with a delimited, database load file that contains the metadata fields listed in Table 1, attached hereto, to the extent already in existence and reasonably accessible or available. The metadata produced should have the correct encoding to enable preservation of the documents' original language. Aside from metadata fields generated during eDiscovery processing and production (e.g., Bates numbers, hash and custodian values, etc.), the producing party is not obligated to produce metadata from a document if the metadata is not already in existence and/or not reasonably accessible or available.

For ESI other than email and e-documents that do not conform to the metadata listed in Table 1, such as text messages, Instant Bloomberg, iMessage, Google Chat, MS Teams, Slack, and Google Docs, the parties agree to meet and confer as to the appropriate metadata fields to be produced.

D. Embedded Objects

Embedded files shall be produced as attachments to the document that contained the embedded file, with the parent/child relationship preserved. The embedded files will be marked with a "YES" in the load file under the "Is Embedded" metadata field. The parties agree logos need not be extracted as separate documents as long as they are displayed in the parent document.

E. Attachments

The parties agree that if any part of a communication or its attachments is responsive, the entire communication and attachments will be produced, except any family member or part thereof that must be withheld or redacted on the basis of privilege. If necessary, the parties will meet and confer about whether there is an appropriate basis for withholding a family document for any reason other than attorney-client or work product privilege. The attachments will be produced sequentially after the parent communication.

The Parties agree to promptly meet and confer regarding the collection and production of hyperlinks containing point-in-time documents in documents and communications in the production population.

F. Compressed Files Types

Compressed file types (*e.g.*, .ZIP, .RAR, .CAB, .Z) should be decompressed so that the lowest level document or file is extracted.

G. Structured Data

To the extent a response to discovery requires production of electronic information stored in a database, the parties agree to meet and confer regarding methods of production.

H. Decryption of Production Data

To the extent there is password or other security protection for a document in a production, the producing party shall produce a slip sheet stating "Technical Issue" (or other similar indicator of a technical problem) and provide the metadata required by Table 1, attached hereto, to the extent it can be reasonably extracted from the file in its encrypted form. If a receiving party believes there is a need to remove the password or other security protection from a document, the receiving party can request it based upon a specific showing of need, and the parties agree to meet and confer in good faith regarding the request. If the Parties cannot resolve their dispute, the objecting party may initiate the Court's process for resolving discovery disputes.

I. Encryption of Data in Transit

Productions will be delivered via secure electronic file transfer protocol system. . To maximize the security of information in transit, any media on which documents being produced are transmitted may be encrypted by the producing party using commercially reasonable encryption technology (e.g., 7-Zip technology). In such cases, the producing party shall transmit the encryption key or password to the receiving party, under separate cover, contemporaneously with sending the encrypted media.

J. Redactions

A party may use redactions to protect for privilege, but shall redact no more than is necessary to protect the relevant privileged information. Each redaction on a document shall be endorsed with the word "redacted," along with the basis for such redaction on the face of the document. (e.g., "Redacted – Attorney Client Privilege"). A producing party need not provide a log entry for a redacted document if the face of the document and the produced metadata provides the information that otherwise would appear on a log and the privilege asserted for the redaction is noted on the face of the document per above. However, if the receiving party is nevertheless unable to determine the basis for the redaction(s), the receiving party may request individual log entry(ies) to determine the basis of such redaction(s).

A party may also redact from any document produced in this action the personal identifying information ("PII") of any person, including but not limited to Social Security numbers, bank account information, and personal health information. To the extent that a receiving party contends that such PII is relevant to the issues presented in this litigation, the Parties agree to meet and confer regarding the production of such PII in a minimally invasive manner. The Parties agree to promptly meet and confer regarding the applicability of and the mechanics of complying with the European Union's General Data Protection Regulation ("GDPR") or other applicable privacy laws.

If documents that the parties have agreed to produce in native format need to be redacted, the parties will implement redactions while ensuring that proper formatting and usability are maintained. Spreadsheets requiring redaction will be redacted using native redaction software and produced in native format.

K. Non-Waiver

Pursuant to Federal Rule of Evidence 502(d), nothing in this Order shall require disclosure of privileged information (i.e., information subject to a claim of attorney-client privilege, work product protection or other privilege or immunity), and the production of privileged information is not a waiver of the privilege or protection from disclosure or discovery in this case or any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d). The provisions of Federal Rule of Evidence 502(b) shall not limit or modify the protections provided above.

L. Privilege Logs

With the exception of privileged documents or work product made after December 7, 2023, for all documents withheld, in whole or in part, on the basis of privilege, the parties agree to furnish logs that comply with the legal requirements under federal law, and the following procedures will apply:

a. The producing party shall be required to produce a limited metadata log for any Discovery Material that the producing party contends is privileged or which the parties agree can be treated as presumptively privileged.

b. For emails, the metadata log shall include the following information (to the extent it is readily ascertainable) date and time sent, email addresses of the sender and recipient(s) (including those copied and blind copied), and subject. To the extent an email sender or recipient cannot be readily identified through his or her email address, the parties may request further identifying information on that individual. No description of the privilege claim is required, except as set forth in subparagraphs (d) and (e) below.

c. For electronic files other than emails, the metadata log shall include the creation date, author, and title of the document, to the extent this information is readily ascertainable. No description of the privilege claim is required, except as set forth in subparagraphs (d) and (e) below. To the extent a party believes in good faith that listing the subject of an email or title of a document on the metadata log would reveal information a party contends is privileged, a description of the privilege claim may be provided in lieu of the email subject or document title.

d. The type of privilege being asserted, such as “AC” for Attorney/Client, “WP” for Attorney Work Product, and “CI” for Common Interest.

e. If discovery materials other than emails and electronic files are included on the limited metadata log, the parties shall meet and confer on the appropriate metadata to include on the log.

f. The parties shall identify on their logs where counsel is present in a conversation.

g. Email thread suppression shall not be used for documents entered into a privilege log.

The parties reserve the right to request that a more detailed document-by-document log be produced for a specific subset of documents, such as documents sent and received during a specific time period, if the receiving party is unable to ascertain the reason for why the document is being withheld as privileged or otherwise protected. If the need arises, the parties agree to meet and confer in good faith regarding the need for a more detailed document-by-document log for a specific subset of documents.

Privilege logs shall be provided in searchable Microsoft Excel format.

Each party shall produce a set of privilege logs, to the extent privileged documents have been withheld from productions, on the following schedule: The first interim log shall be produced 60 days before substantial completion of document productions. The second shall be produced 14 days before substantial completion. The final log shall be produced 14 after substantial completion. When a party provides multiple, or supplemental, privilege logs, each such log should contain all previous privilege log entries, such that each privilege log can supersede all prior privilege logs, with any changes to previously produced privilege log entries clearly identified.

Documents presumptively not to be logged on a privilege log include: communications exclusively between a party or its representative(s) and its trial counsel for this matter, after the commencement of this litigation on December 7, 2023; and/or work product created by counsel, an agent of counsel, or a party at the direction of counsel, for this matter, after commencement of this litigation on December 7, 2023.

DATED: April 28, 2025

LABATON KELLER SUCHAROW LLP

By: *<u>/s/ James T. Christie</u>*
Michael P. Canty
James T. Christie
Guillaume Buell
Jacqueline R. Meyers
140 Broadway
New York, New York 10005
Telephone: 212-907-0700
Facsimile: 212-818-0477
Email: mcanty@labaton.com
jchristie@labaton.com
gbuell@labaton.com
jmeyers@labaton.com

Lead Counsel for Lead Plaintiff Macomb County Employees' Retirement System, Macomb County Retiree Health Care Fund, and Wayne County Employees' Retirement System and the Proposed Class

VANOVERBEKE MICHAUD & TIMMONY P.C.
Thomas C. Michaud (*pro hac vice* forthcoming)
79 Alfred Street
Detroit, Michigan 48201
Telephone: (313) 578-1200
Facsimile: (313) 578-1201
Email: tmichaud@vmtlaw.com

Liaison Counsel for Lead Plaintiff Macomb County Employees' Retirement System, Macomb County Retiree Health Care Fund, and Wayne County Employees' Retirement System and the Proposed Class

GIBSON, DUNN & CRUTCHER LLP

By: *<u>/s/ Monica K. Loseman</u>*
Barry H. Berke
Mary Beth Maloney
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.3860
Facsimile: 212.817.9230
BBerke@gibsondunn.com
MMaloney@gibsondunn.com

Jason J. Mendro
1700 M Street, N.W.
Washington, D.C. 20036-4504
Telephone: 202.887.3726
Facsimile: 202.530.9626
JMendro@gibsondunn.com

Monica K. Loseman (*pro hac vice*)
1900 Lawrence Street
Suite 3000
Denver, CO 80202-2211
Telephone: 303.298.5784
Facsimile: 303.313.2828
MLoseman@gibsondunn.com

Counsel for Defendants The Estée Lauder Companies Inc., Fabrizio Freda, and Tracey T. Travis

IT IS SO ORDERED.

Date: April 29, 2025

Hon. Arun Subramanian
United States District Judge

TABLE 1: METADATA FIELDS[1]

Field Name	Example / Format	Description
BEGNO / PRODBEG	ABC0000001 (Unique ID)	The Document ID number associated with the first page of a document.
ENDNO / PRODEND	ABC0000003 (Unique ID)	The Document ID number associated with the last page of a document.
BEGATTACH	ABC0000001 (Unique ID Parent-Child Relationships)	The Document ID number associated with the first page of the parent document.
ENDATTACH	ABC0000008 (Unique ID Parent-Child Relationships)	The Document ID number associated with the last page of the last attachment.
CONFIDENTIALITY DESIGNATION	Confidential; Highly Confidential	If document assigned confidentiality by Counsel
PGCOUNT	Numeric	The number of pages in a document (image records)
SOURCE	Joe Smith Office; HR File Room	Location where hard-copy documents were found at time of collection.
VOLUME	VOL001	The name of CD, DVD, or Hard Drive.
RECORDTYPE	Email, Attachment, Scanned Doc, eFile, Chat/Text	The record type of a document.
SENTDATE	MM/DD/YYYY	The date the email or calendar entry was sent.
SENTTIME	HH:MM	The time the email or calendar entry was sent.
RECEIVEDDATE	MM/DD/YYYY	The date the document was received.
RECEIVEDTIME	HH:MM	The time the document was received.
CREATEDATE	MM/DD/YYYY	The date the document was created.
CREATETIME	HH:MM	The time the document was created.
LASTMODDATE	MM/DD/YYYY	The date the document was last modified.
LASTMODTIME	HH:MM	The time the document was last modified.
FILE LAST ACCESS DATE	MM/DD/YYYY	The date the document was last accessed.
FILE LAST SAVED BY	jsmith	The last individual to save the file.
FILE LAST EDITED BY	jsmith	The name of the last person to edit the document from extracted metadata.
MEETING START DATE	MM/DD/YYYY	Start date of calendar entry.
MEETING START TIME	HH:MM	Start time of calendar entry.
MEETING END DATE	MM/DD/YYYY	End date of calendar entry.
MEETING END TIME	HH:MM	End time of calendar entry.
FILEPATH	/JsmithPC/Users/Jsmith/Desktop	The file path from the location in which the document was stored in the usual course of business. This field should be populated for

[1] For ESI other than email and e-docs that do not conform to the metadata listed here, such as text messages, Instant Bloomberg, iMessage, Google Chat, MS Teams, and Slack, the parties will meet and confer as to the appropriate metadata fields to be produced (as provided in Section III.A, *supra*).

		both email and e-files.
FILEPATH-DUP	/JSmith.pst/Inbox/Network Share/Accounting/… /TJohnsonPC/Users/TJohnson/My Documents/...	The file paths from the locations in which the duplicate documents were stored in the usual course of business. This field should be populated for both email and e-files and separated by semicolons.
FILE SIZE	Numeric	The file size of a document (including embedded attachments).
AUTHOR	jsmith	The author or owner of a document from extracted metadata.
LASTEDITEDBY	jsmith	The name of the last person to edit the document from extracted metadata.
FROM	Joe Smith <jsmith@email.com>	The display name and email address of the author of an email/calendar item. An email address should always be provided.
TO	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and email address of the recipient(s) of an email/calendar item. An email address should always be provided for every email if a recipient existed.
CC	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and email of the copyee(s) of an email/calendar item. An email address should always be provided for every email if a copyee existed.
BCC	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and email of the blind copyee(s) of an email or calendar item. An email address should always be provided for every email if a blind copyee existed.
SUBJECT		The subject line of the email/calendar item.
MESSAGE TYPE	Appointment, Contact, Task, Distribution List, Message, etc.	An indication of the email system message type.
IMPORTANCE	Normal, Low, High	Email Importance Flag
TITLE		The extracted document title of a document.
CUSTODIAN-ALL	Smith, Joe; Doe, Jane	All of the custodians of a document from which the document originated, separated by semicolons.
SOURCE	Computer, Mobile Phone, Email, Network Share, Slack, WhatsApp, Teams, Database Name, etc.	The source from which the document was collected.
ATTACH COUNT	Numeric	The number of attachments to a document.
ATTACHMENT NAME	Attach1.doc	The original file name of an attached document.
FILEEXT	XLS	The file extension of a document.
FILENAME	Document Name.xls	The file name of a document.
FILE MANAGER / APPLICATION DESCRIPTION	Microsoft Excel, Word, etc.	Native file application.
FILESIZE	Numeric	The file size of a document (including embedded attachments).
TRACK CHANGES	Yes or No	The yes/no indicator of whether tracked changes exist in the file.
IS EMBEDDED	Yes or No	The yes/no indicator of whether a file is embedded in another document.

HASH		The MD5 or SHA-1 Hash value or "de-duplication key" assigned to a document. The same hash method (MD5 or SHA-1) should be used throughout production.
CONVERSATION INDEX		ID used to tie together email threads.
REDACTED	Yes or Blank	If a document contains a redaction, this field will display 'Yes'.
TIMEZONE PROCESSED	PST, CST, EST, etc	The time zone the document was processed in. **NOTE:** This should be the time zone where the documents were located at time of collection.
NATIVELINK	D:\NATIVES\ABC000001.xls	The full path to a native copy of a document.
FULLTEXT	D:\TEXT\ABC000001.txt	The path to the full extracted text of the document. There should be a folder on the deliverable, containing a separate text file per document. These text files should be named with their corresponding Bates numbers. **Note**: Emails should include header information: author, recipient, cc, bcc, date, subject, etc. If the attachment or e-file does not extract any text, then OCR for the document should be provided.